# BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

## IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.**

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 44 08 603 A 1**

(51) Int. Cl.[6]:
**G 05 B 19/048**
G 05 B 9/02

(21) Aktenzeichen: P 44 08 603.2
(22) Anmeldetag: 8. 3. 94
(43) Offenlegungstag: 14. 9. 95

DE 44 08 603 A 1

(71) Anmelder:
Mannesmann AG, 40213 Düsseldorf, DE

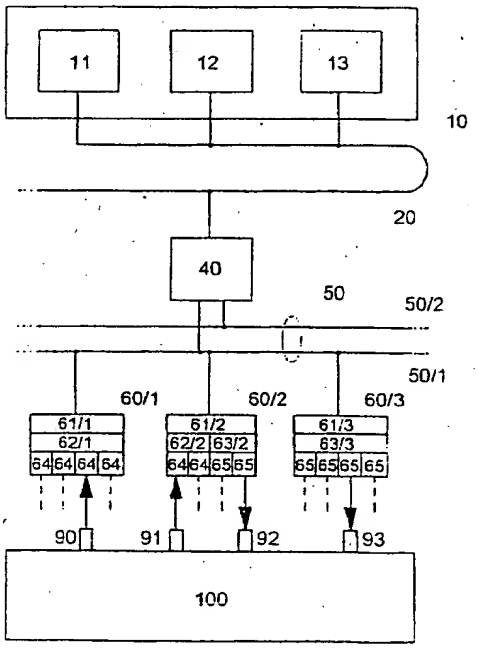
(74) Vertreter:
P. Meissner und Kollegen, 14199 Berlin

(72) Erfinder:
Albrecht, Dieter, 65187 Wiesbaden, DE

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zur Erhöhung der Sicherheit in hierarchisch strukturierten Automatisierungssystemen

(57) Die Erfindung betrifft ein Verfahren zur Erhöhung der Sicherheit in hierarchisch strukturierten und konfigurierbaren Automatisierungssystemen zur Steuerung und Regelung technischer Prozesse in der Automatisierungstechnik mit mindestens einer zentralen Verarbeitungseinrichtung (40) und einer Mehrzahl an diese angeschlossene Eingabe-/Ausgabeeinrichtungen (60/1 bis 60/3) oder einer angeschlossenen Eingabe-/Ausgabeeinrichtung (60/2) mit einer Mehrzahl Eingabe- und/oder Ausgabeschnittstellen (64, 65). Um zu verhindern, daß Bedienfehler, Fehler durch Betriebseinflüsse Konfigurier- und Parametrierfehler in komplexen Automatisierungssystem auf den zu automatisierenden Prozeß durchgreifen, wird vorgeschlagen, mit einer zentralen Verarbeitungseinrichtung (40) prozeßglobale Steuerungssequenzen in Abhängigkeit von prozessualen Meßwerten und vorkonfigurierbaren Führungsgrößen zu erzeugen und Stellwerte auszugeben. Darüber hinaus werden in den Controllern (61/1 bis 61/3) der angeschlossenen Eingabe-/Ausgabeeinrichtungen (60/1 bis 60/3) jeweils lokale Grenzwerte und unzulässige Stellwertkombinationen statisch hinterlegt, eingehende Stellwerte mit den lokalen Grenzwerten und unzulässigen Stellwertkombinationen verglichen und unzulässige Stellwerte gegen zulässige Ersatzstellwerte ausgetauscht.




DE 44 08 603 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

## Beschreibung

Die Erfindung betrifft ein Verfahren zur Erhöhung der Sicherheit in hierarchisch strukturierten und konfigurierbaren Automatisierungssystemen zur Steuerung und Regelung technischer Prozesse in der Automatisierungstechnik mit mindestens einer zentralen Verarbeitungseinrichtung und einer Mehrzahl an dieser angeschlossener Eingabe-/Ausgabeeinrichtungen oder einer angeschlossenen Eingabe-/Ausgabe-Einrichtung mit einer Mehrzahl Eingabe- und/oder Ausgabeschnittstellen.

Für die Auslegung von automatisierungstechnischen Anlagen unter sicherheitstechnischem Aspekt ist es allgemein bekannt, zwei oder mehr identische Systeme oder Subsysteme parallel zueinander zu konfigurieren und zu betreiben. Bei Ausfall eines Systems oder Subsystems tritt eines der parallel angeordneten Redundanten-Systeme oder Subsysteme an dessen Stelle, ohne daß der technische Prozeß unterbrochen werden muß. Jedes Steuerungssubsystem ist dabei gemäß "Automatisierungstechnik", Band 1, insbesondere Seite 162, R. Oldenbourgverlag München Wien 1992, sowohl für die Signalaufbereitung und die Regelung als auch für die Überwachung ausgelegt. Derartig redundante Ausgestaltungen dienen der Erhöhung der Verfügbarkeit des Automatisierungssystems. Da die redundanten Komponenten physisch mehrfach in identischer Ausführung vorhanden sind und während der ausfallfreien Betriebszeit nicht zur Lösung der automatisierungstechnischen Aufgabe beitragen, werden die damit verbundenen technischen Mehraufwendungen trotz des sicherheitsrelevanten Erfordernisses als nachteilig angesehen.

Es ist weiterhin bekannt und in den Normen DIN V 0801 und DIN V 19250 manifestiert, daß eine Erhöhung der Sicherheit eines Automatisierungssystems durch eine Mehrzahl physisch und logisch unterschiedlicher Steuerungssubsysteme zu realisieren, die sich, bezogen auf denselben technischen Prozeß oder einen Teil davon, ergänzen oder überwachen. Die Überwachung kann dabei einseitig oder gegenseitig erfolgen. Da, bezogen auf eine beliebige Prozeßvariable, jedes speziell ausgeprägte Subsystem ausschließlich singulär vorliegt, wird diese Struktur als diversitäre Teilredundanz bezeichnet. Physisch liegen dabei weiterhin mindestens zwei separate Subsysteme vor.

Mit zunehmender Komplexität automatisierungstechnischer Einrichtungen und aufgrund wachsender Datentransferraten sind periphere Einrichtungen, insbesondere Eingabe-/Ausgabeeinrichtungen in zunehmendem Maße mit signalverarbeitenden Mitteln, sogenannten Controllern, ausgestattet. Diese Controller dienen dem zeitgeteilten Zugriff auf gemultiplexte Datenkanäle zum Empfang und Senden von Daten und Steuerinformationen der jeweils zugeordneten Einrichtung und der Ansteuerung der zugehörigen Dateneinn- und Datenausgabeschnittstellen.

Der Erfindung liegt daher die Aufgabe zugrunde, die Sicherheit in einem hierarchisch strukturierten konfigurierbaren Automatisierungssystem der eingangs beschriebenen Art zu erhöhen, ohne dabei den materiellen Aufwand zu erhöhen. Insbesondere soll verhindert werden, daß Bedienfehler, Fehler durch Betriebseinflüsse, Konfigurier- und Parametrierfehler in komplexen Automatisierungssystemen auf den zu automatisierenden Prozeß durchgreifen.

Diese Aufgabe wird erfindungsgemäß mit den Mitteln des Patentanspruchs 1 gelöst. Weiterführende vorteilhafte Ausgestaltungen der Erfindung sind in den Patentansprüchen 2 bis 6 beschrieben.

Die Erfindung wird nachstehend anhand von Ausführungsbeispielen näher erläutert. Die dazu erforderlichen Zeichnungen zeigen:

Fig. 1 eine Darstellung einer hierarchischen Systemarchitektur eines Automatisierungssystems,

Fig. 2 eine Darstellung der zeitlichen Controlleraktivität zum Datentransfer bei einem Datenkanal,

Fig. 3 eine Darstellung der zeitlichen Controlleraktivität bei mehreren Datenkanälen.

In Fig. 1 ist ein hierarchisch strukturiertes Automatisierungssystem dargestellt, das mindestens eine zentrale Verarbeitungseinheit 40 aufweist, die über einen Systembus 20 an in einem Wartenbereich 10 angeordnete Bedieneinrichtungen 11, Beobachtungseinrichtungen 12 und Konfiguriereinrichtungen 13 angeschlossen sind. Die zentrale Verarbeitungseinrichtung 40 ist über mindestens einen Datenkanal 50/1 mit einer Mehrzahl Eingabe-/Ausgabeeinrichtungen 60/1 bis 60/3 verbunden, die zur Koordinierung des Datenaustauschs mit der zentralen Verarbeitungseinrichtung 40 jeweils einen Controller 61/1 bis 61/3 aufweisen. Jede Eingabe-/Ausgabeeinrichtung 60/1 bis 60/3 ist jeweils als austauschbare physische Einheit ausgeführt. Jede physische Eingabe-/Ausgabeeinrichtung 60/1 bis 60/3 kann logisch als reine Dateneingabeeinrichtung, als reine Datenausgabeeinrichtung oder als gemischte Dateneingabe- und Datenausgabeeinrichtung ausgeführt sein. In Fig. 1 ist die Eingabe-/Ausgabeeinrichtung 60/1 als reine Dateneingabeeinrichtung 62/1 dargestellt und ausschließlich mit Eingabeschnittstellen 64 ausgestattet. Weiterhin ist in Fig. 1 die Eingabe-/Ausgabeeinrichtung 60/3 als reine Datenausgabeeinrichtung 63/3 dargestellt, die ausschließlich mit Ausgabeschnittstellen 65 ausgestattet ist. Die Eingabe-/Ausgabeeinrichtung 60/2 weist eine Dateneingabeeinrichtung 52/2 und eine Datenausgabeeinrichtung 63/2 auf. Der Dateneingabeeinrichtung 62/2 sind Eingabeschnittstellen 64 zugeordnet, und der Datenausgabeeinrichtung 63/2 sind Ausgabeschnittstellen 65 zugeordnet.

Weiterhin sind in Fig. 1 Meßwertgeber 90 und 91 und Stellglieder 92 und 93 dargestellt, die an einen Prozeß 100 adaptiert sind. Der Meßwertgeber 90 ist mit einer der Eingabeschnittstellen 64 der Dateneingabeeinrichtung 62/1 und der Meßwertgeber 91 ist mit einer der Eingabeschnittstellen 64 der Dateneingabeeinrichtung 62/2 verbunden. An eine der Ausgabeschnittstellen 65 der Datenausgabeeinrichtung 63/2 ist das Stellglied 92, und an eine der Ausgabeschnittstellen 65 der Datenausgabeeinrichtung 63/3 ist das Stellglied 93 angeschlossen.

In Fig. 2 ist der zeitliche Ablauf des Zugriffs der zentralen Verarbeitungseinrichtung 40 auf dem Datenkanal 50/1 anhand zyklisch wechselnden Zugriffs auf die Eingabe-/Ausgabeeinrichtungen 60/1 bis 60/3, die repräsentiert sind durch ihre Controller 61/1 bis 61/3, dargestellt. Während der mit T1 bezeichneten Perioden ist ein Datenaustausch zwischen der zentralen Verarbeitungseinrichtung 40 und dem Controller 61/1 der Eingabe-/Ausgabeeinrichtung 60/1 vorgesehen. Während der Zeitphasen T2 und T3 erfolgt der Datenaustausch zwischen der zentralen Verarbeitungseinrichtung 40 und den Controllern 61/2 und 61/3 der Eingabe-/Ausgabeeinrichtung 60/2 und 60/3. Durch den wechselweisen Zugriff ist der Controller 61/1 während der Zeitphasen T2 und T3, der Controller 61/2 während der Zeitphasen T3 und T1 und der Controller 61/3 während der Zeitphasen T1 und T2 vom Datentransfer freigestellt.

Prozessuale Meßwerte werden an den Meßwertge-

bern 90 und 91 aufgenommen, über die Eingabeschnittstellen 64 der Dateneingabeeinrichtungen 62/1 und 62/2 eingelesen und während zugeordneter Zeitphasen T1 bzw. T2 an die zentrale Verarbeitungseinrichtung 40 übertragen. In Abhängigkeit von den prozessualen Meßwerten und vorkonfigurierbaren Führungsgrößen werden mit der zentralen Verarbeitungseinrichtung 40 prozeßglobale Steuerungssequenzen erzeugt und während zugeordneter Zeitphasen T2 bzw. T3 an die Datenausgabeeinrichtungen 63/2 und 63/3 übertragen. Die Stellwerte werden über die Ausgabeschnittstellen 65 an die Stellglieder 92 und 93 ausgegeben.

In den Controllern 61/2 und 61/3 der Datenausgabeeinrichtungen 63/2 und 63/3 sind jeweils lokale Grenzwerte und unzulässige Stellwertkombinationen statisch hinterlegbar. Während controllerindividuellen Perioden ruhenden Datenverkehrs, für den Controller 61/2 sind das die Perioden T3 und T1, werden die eingehenden Stellwerte mit den lokalen Grenzwerten und unzulässigen Stellwertkombinationen verglichen und unzulässige Stellwerte gegen zulässige Ersatzstellwerte ausgetauscht. Dabei ist sowohl vorgesehen, daß als Ersatzstellwerte die letzten zulässigen Stellwerte gehalten werden, als auch daß bei der Systeminitialisierung Ersatzstellwerte vorgegeben werden. Darüber hinaus ist vorgesehen, Ersatzstellwerte aus eingehenden Meßwerten zu berechnen.

Für Eingabe-/Ausgabeeinrichtungen 60/2, die mit einer Dateneingabeeinrichtung 62/2 und einer Datenausgabeeinrichtung 63/2 ausgestattet sind, ist darüber hinaus vorgesehen, die vorgegebenen lokalen Grenzwerte und unzulässige Stellwertkombinationen mit eingehenden Meßwerten zu korrelieren, um so unzulässige Stellwertkombinationen und lokale Grenzwerte dynamisch auszuwählen oder dynamisch zu bilden und eingehende Stellwerte mit den entstandenen dynamischen Grenzwerten und unzulässigen Stellwertkombinationen zu vergleichen. Stellwertkombinationen umfassen dabei die Kombination von Binärwerten bzw. von Zuständen, die an binären Ausgabe- oder Eingabeschnittstellen 64, 65 anliegen. Grenzwerte beziehen sich auf analoge Größen und ihre Darstellung.

Darüber hinaus kann ein Automatisierungssystem gemäß **Fig.** 1 mit einer Mehrzahl von Datenkanälen 50/1 und 50/2 die zu einer Gruppe 50 zusammengefaßt sind, ausgestattet sein. Die Datenkanäle 50/1 und 50/2 der Gruppe 50 sind jeweils an die zentrale Verarbeitungseinheit 40 angeschlossen. An den Datenkanal 50/2 sind weitere in **Fig.** 1 nicht dargestellte Eingabe-/Ausgabeeinrichtungen angeschlossen. Die Datenkanäle 50/1 und 50/2 der Gruppe 50 werden gemäß **Fig.** 3 wechselweise zum Datenaustausch zwischen der zentralen Verarbeitungseinrichtung 40 und angeschlossenen Eingabe-/Ausgabeeinrichtungen beaufschlagt. Während der Zeitphasen T1, T3 und T5 erfolgt dabei in Analogie zur Darstellung in **Fig.** 2 der Datenaustausch zwischen der zentralen Verarbeitungseinrichtung 40 und den an den Datenkanal 50/1 angeschlossenen Eingabe-/Ausgabeeinrichtungen 60/1 bis 60/3. Durch den wechselweisen Datentransfer unter Einbeziehung der zentralen Verarbeitungseinheit 40 über die Datenkanäle 50/1 und 50/2 ist während der Zeitphasen T2, T4 und T6 der Datenkanal 50/1 zunächst datenfrei. Während dieser Zeitphasen kann vorgesehen sein, daß Eingabe-/Ausgabeeinrichtungen 60/1 bis 60/3 paarweise untereinander über den Datenkanal 50/1 Informationen austauschen.

Dadurch ist es möglich, mit den Controllern 61/2 und 61/3 der Eingabe-/ Ausgabeeinrichtungen 60/2 und 60/3, die Datenausgabeeinrichtungen 63/2 und 63/3 aufweisen, von der zentralen Verarbeitungseinrichtung 40 eingehende Stellwerte mit dynamischen ausgewählten oder erzeugten Grenzwerten und unzulässigen Stellwertkombinationen zu vergleichen, die durch Korrelation von vorgegebenen lokalen Grenzwerten und unzulässigen Stellwertkombinationen und eingehenden Stellwerten und Grenzwerten physisch getrennter Eingabe-/Ausgabeeinrichtungen 60/1 und 60/2 vorgegeben werden.

In einfachster Ausprägung wird dazu für eine reine Datenausgabeeinrichtung 63/3 ohne Datenaustausch mit anderen Eingabe-/ Ausgabeeinrichtungen 60/1 und 60/2 die Wahrheitstabelle, die alle möglichen Ausgabezustände dieser Datenausgabeeinrichtung 63/3 umfaßt, um eine Kennzeichnung der unzulässigen Zustände erweitert und im Controller 61/3 hinterlegt.

Soweit Datenaustausch zwischen den Eingabe-Ausgabeeinrichtungen 60/1 bis 60/3 vorgesehen ist, umfaßt die Wahrheitstabelle darüber hinaus Ausgangszustände physisch benachbarter Datenausgabeeinrichtungen und durch Meßwerte injizierte Eingangszustände physisch benachbarter Dateneingabeeinrichtungen. Dabei werden darüber hinaus unzulässige dynamische Kombinationen von Eingangszuständen und Ausgangszuständen gekennzeichnet und in den Controllern 61/2 und 61/3 der zugeordneten Datenausgabeeinrichtungen 63/2 und 63/3 hinterlegt. Physisch benachbarte Datenausgabeeinrichtungen 63/2 und 63/3 sind dabei solche, die an denselben Datenkanal 50/1 oder 50/2 angeschlossen sind oder Daten unter Umgehung der zentralen Verarbeitungseinheit 40 austauschen können.

In weiterer Ausgestaltung der Erfindung werden den lokalen Grenzwerten und den zulässigen Stellwerten bzw. Stellwertkombinationen Kennungen zugeordnet. Für die Korrelation lokaler Grenzwerte und unzulässiger Stellwertkombinationen mit denen physisch benachbarter Datenausgabeeinrichtung 63/2 und 63/3 genügt es, dazu die Kennungen auszutauschen. Auf diese Weise läßt sich die Belegungszeit des angeschlossenen Datenkanals 50/1 oder 50/2 reduzieren.

In besonderer Ausgestaltung der Erfindung werden ausschließlich mit Kennungen versehene lokale Grenzwerte und unzulässige Stellwertkombinationen im jeweiligen Controller 61/1 bis 61/3 hinterlegt. Vorteilhafterweise ist dabei der erforderliche Speicherplatz auf ein Minimum reduzierbar.

In vorteilhafter Weise ist die logische Überwachung der Stellwerte auf Überschreitung von lokalen Grenzwerten und unzulässigen Stellwertkombinationen logisch von der zentralen Verarbeitungseinheit 40 getrennt, so daß trotz Singularität sowohl der zentralen Verarbeitungseinheit 40 als auch aller angeschlossener Eingabe-/Ausgabeeinrichtungen 60/1 bis 60/3 bei Ausfall der zentralen Verarbeitungseinheit 40 der Prozeß 100 in einen gefahrlosen Zustand gesteuert wird, ohne dabei weiteren materiellen Aufwand vorsehen zu müssen. Weiterhin ist aufgrund der geringen Funktionalität der verfahrenstechnischen Maßnahmen in den Controllern 61/1 bis 61/3 die Störanfälligkeit des jeweiligen Überwachungssystems sehr gering. Darüber hinaus lassen sich Handhabungsfehler in der Bedienung des Prozesses sowie Konfigurier- und Parametrierfehler auf den angeschlossenen Prozeß vermeiden.

Bezugszeichenliste

10 Wartenbereich

11 Bedieneinrichtung
12 Beobachtungseinrichtung
13 Konfiguriereinrichtung
20 Systembus
40 zentrale Verarbeitungseinrichtung
50 Gruppe
50/1, 50/2 Datenkanal
60/1—60/3 Eingabe-Ausgabeeinrichtungen
61/1—61/3 Controller
62/1, 62/2 Dateneingabeeinrichtung
63/2, 63/3 Datenausgabeeinrichtung
64 Eingabeschnittstellen
65 Ausgabeschnittstellen
90, 91 Meßwertgeber
92, 93 Stellglieder
100 Prozeß.

## Patentansprüche

1. Verfahren zur Erhöhung der Sicherheit in hierarchisch strukturierten Automatisierungssystemen zur Steuerung und Regelung technischer Prozesse mit mindestens einer zentralen Verarbeitungseinrichtung und einer Mehrzahl an dieser angeschlossener Eingabe-/Ausgabeschnittstellen, wobei die Eingabe-/Ausgabeschnittstellen einzeln oder gruppenweise mit von der zentralen Verarbeitungseinrichtung unabhängigen Controllern ausgestattet sind, **dadurch gekennzeichnet,**
   - daß mit der zentralen Verarbeitungseinrichtung (40) prozeßglobale Steuerungssequenzen in Abhängigkeit von prozessualen Meßwerten und vorkonfigurierbaren Führungsgrößen erzeugt und Stellwerte ausgegeben werden,
   - daß in den Controllern (61/1 bis 61/3) jeweils lokale Grenzwerte und unzulässige Stellwertkombinationen statisch hinterlegt werden, eingehende Stellwerte mit den lokalen Grenzwerten und unzulässigen Stellwertkombinationen verglichen werden und unzulässige Stellwerte gegen zulässige Ersatzstellwerte ausgetauscht werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß als Ersatzstellwerte die letzten zulässigen Stellwerte gehalten werden.
3. Verfahren nach Anspruch 1, dadurch gekennzeichnet daß bei der Systeminitialisierung Ersatzstellwerte vorgegeben werden.
4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Ersatzstellwerte aus eingehenden Meßwerten berechnet werden.
5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß die lokalen Grenzwerte und unzulässigen Stellwertkombinationen durch Korrelation mit eingehenden Meßwerten dynamisch festgelegt werden.
6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß die Stellwerte mehrerer physisch separater Datenausgabeeinrichtungen (63/2 und 63/3) zur Festlegung der Grenzwerte und der Unzulässigkeit von Stellwertkombinationen miteinander korreliert werden.
7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Stellwerte mit Meßwerten mehrerer physisch separater Dateneingabeeinrichtungen (62/1 und 62/2) zur Festlegung der Grenzwerte und der Unzulässigkeit von Stellwertkombinationen korreliert werden.
8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß die aktuellen Grenzwerte und unzulässigen Stellwertkombinationen aus der Menge der Meßwerte, der Stellwerte und der vorgegebenen Grenzwerte dynamisch berechnet werden.

Hierzu 2 Seite(n) Zeichnungen

Nummer: DE 44 08 603 A1
Int. Cl.[6]: G 05 B 19/048
Offenlegungstag: 14. September 1995

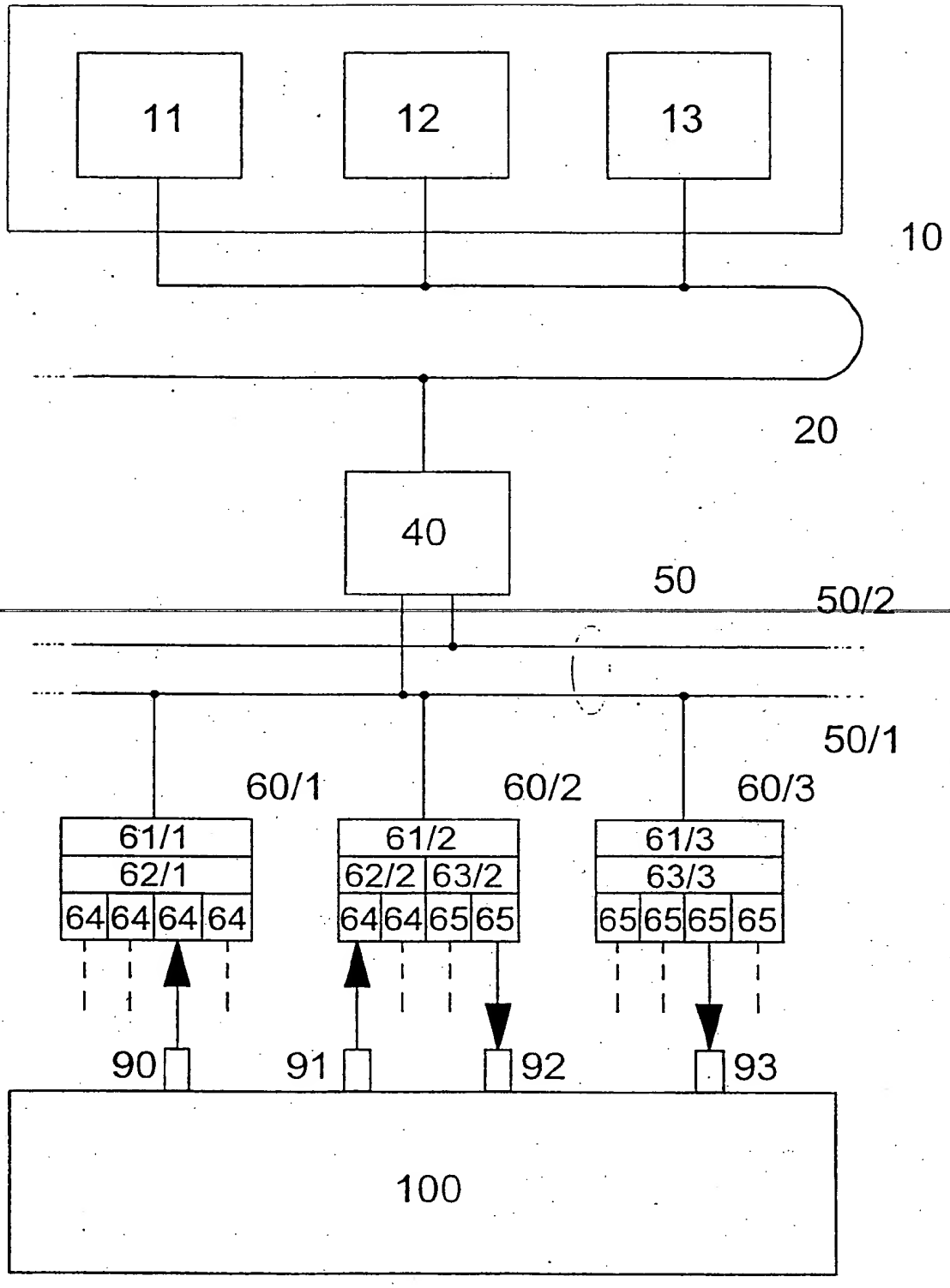



Fig. 1

Nummer: DE 44 08 603 A1
Int. Cl.[6]: G 05 B 19/048
Offenlegungstag: 14. September 1995

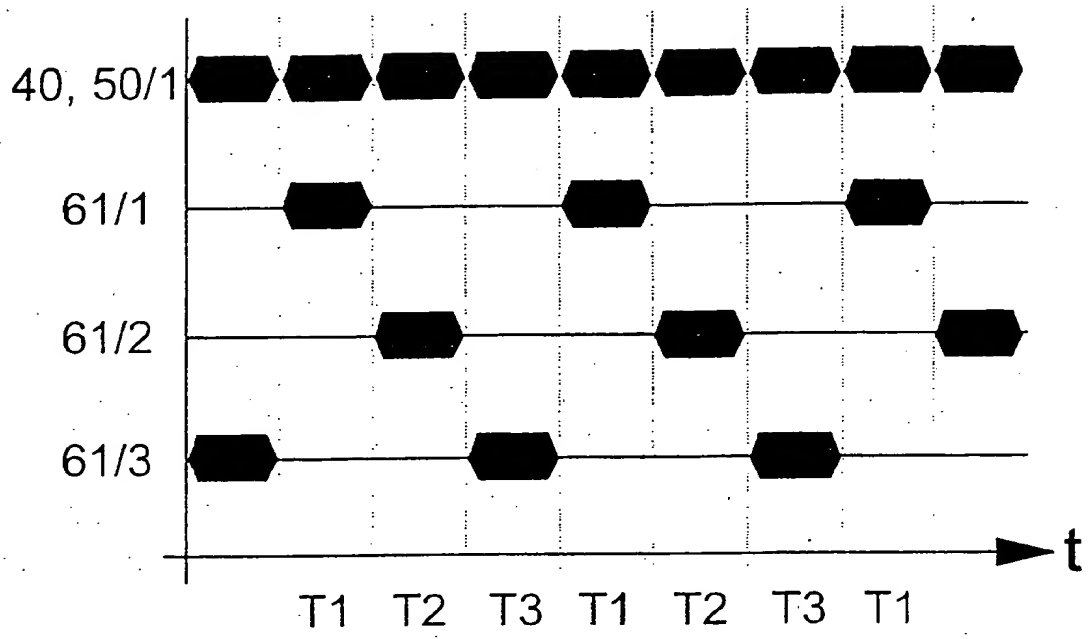



Fig. 2

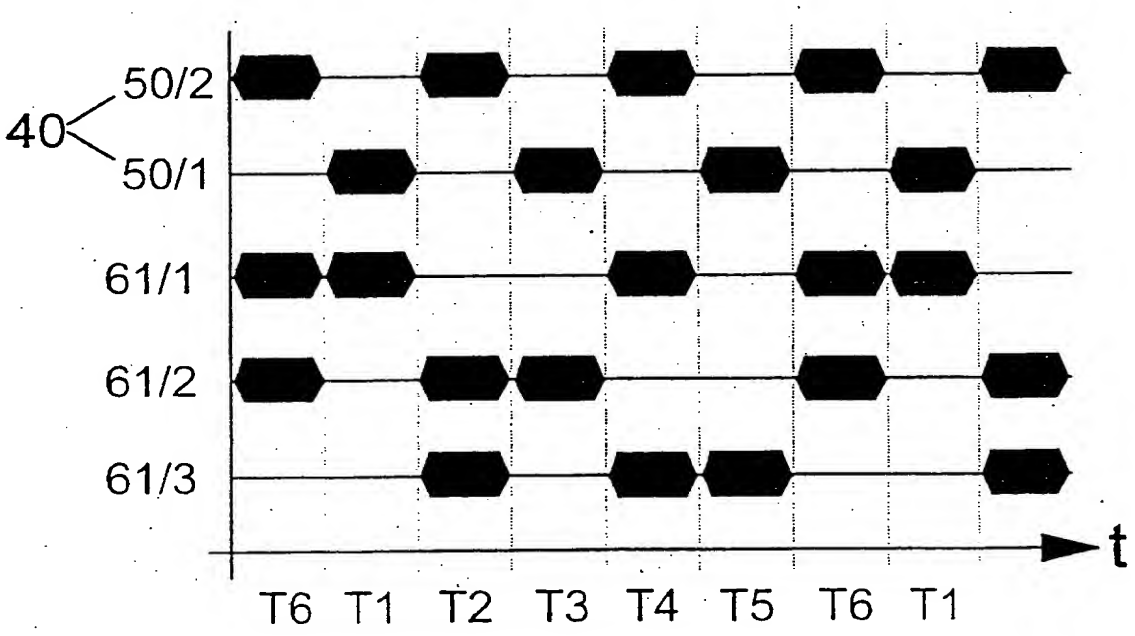



Fig. 3

# Increase of security of hierarchically structured automation systems

Patent Number: DE4408603
Publication date: 1995-09-14
Inventor(s): ALBRECHT DIETER (DE)
Applicant(s): MANNESMANN AG (DE)
Requested Patent: ☐ DE4408603
Application Number: DE19944408603 19940308
Priority Number(s): DE19944408603 19940308
IPC Classification: G05B19/048; G05B9/02
EC Classification: G05B9/02, G05B15/02
Equivalents:

## Abstract

A central processor (40) is connected by a system bus (20) to operating, monitoring and configuration devices (11-13) in an administrative area (10), and by data channels (50) to a number of input/output devices (60/1-60/3) with controllers (61) for coordination of data exchange. Overall process control sequences are produced in accordance with measured values and pre-configurable control quantities. Local limits and forbidden combinations of settings are statically stored in the controllers for comparison with incoming settings. Allowable settings are substituted for any which are excluded by the comparison.

DOCKET NO: J&R-0724
SERIAL NO: 09/918,423
APPLICANT: von Wendorff

LERNER AND GREENBERG P.A.
P.O. BOX 2480
HOLLYWOOD, FLORIDA 33022
TEL. (954) 925-1100